BESCHWERDEKAMMERN DES EUROPÄISCHEN PATENTAMTS

BOARDS OF APPEAL OF THE EUROPEAN PATENT OFFICE

CHAMBRES DE RECOURS DE L'OFFICE EUROPEEN DES BREVETS

Internal distribution code:
(A) [ ] Publication in OJ
(B) [ ] To Chairmen and Members
(C) [ ] To Chairmen
(D) [X] No distribution

D E C I S I O N
of 11 July 2003

Case Number: T 0611/99 - 3.4.1

Application Number: 89302812.6

Publication Number: 0334616

IPC: G07F 7/10

Language of the proceedings: EN

Title of invention:
Method and system for personal identification

Patentee:
POLAROID CORPORATION

Opponent:
GIESECKE & DEVRIENT GmbH

Headword:
-

Relevant legal provisions:
EPC Art. 52(1), 56, 100(a)

Keyword:
"Inventive step (no)"

Decisions cited:
-

Catchword:
-

Europäisches Patentamt | European Patent Office | Office européen des brevets

Beschwerdekammern | Boards of Appeal | Chambres de recours

Case Number: T 0611/99 - 3.4.1

D E C I S I O N
of the Technical Board of Appeal 3.4.1
of 11 July 2003

Appellant: (Proprietor of the patent)
POLAROID CORPORATION
549 Technology Square
Cambridge
Massachusetts 02139 (US)

Representative:
Skone James, Robert Edmund
GILL JENNINGS & EVERY
Broadgate House
7 Eldon Street
London EC2M 7LH (GB)

Respondent: (Opponent)
GIESECKE & DEVRIENT GmbH
Prinzregentenstrasse 159
D-81677 München (DE)

Representative:
Schmitt-Nilson, Gerhard
Klunker Schmitt-Nilson Hirsch
Winzererstrasse 106
D-80797 München (DE)

Decision under appeal:
Decision of the Opposition Division of the European Patent Office posted 6 April 1999 revoking European patent No. 0334616 pursuant to Article 102(1) EPC.

Composition of the Board:

Chairman: G. Davis
Members: R. Q. Bekkering
G. Assi

Summary of Facts and Submissions

I. The appellant (patentee) lodged an appeal against the decision of the opposition division, dispatched on 6 April 1999, revoking the European patent No. 0 334 616. The notice of appeal was received on 4 June 1999, the appeal fee being paid on the same day, and the statement of grounds of appeal was received on 13 August 1999.

II. Opposition had been filed against the patent as a whole, based on Article 100(a) EPC on the ground of lack of inventive step (Articles 52(1), 56 EPC).

The opposition division held that independent claim 6 as granted did not involve an inventive step and revoked the patent accordingly.

The appellant requested that the decision under appeal be set aside and the patent be maintained in amended form on the basis of:

Main request:

Claims: No. 1 to 3 and 4 (part) as granted
No. 4(part) and 5 to 7 filed with letter of 13 August 1999

Description: columns 1, 2 and 5 to 11 as granted
columns 3, 4 filed with letter of of 13 August 1999

Figures: pages 13 to 15 of the patent specification

First auxiliary request:

Claims: No. 1 to 3 and 4 (part) as granted
No. 4(part) and 5 to 7 filed with letter of 13 August 1999

Description: columns 1, 2 and 5 to 11 as granted
columns 3, 4 filed with letter of 13 August 1999

Figures: pages 13 to 15 of the patent specification

Second auxiliary request:

Claims: No. 1 to 3 and 4 (part) as granted
No. 4(part) and 5 filed with letter of 13 August 1999

Description: columns 1, 2 and 5 to 11 as granted
columns 3, 4 filed with letter of 13 August 1999

Figures: pages 13 to 15 of the patent specification

Third auxiliary request:

Claims: No. 1 to 3 filed with letter of 13 August 1999

Description: columns 1, 2 and 5 to 11 as granted
columns 3, 4 filed with letter of 13 August 1999

Figures: pages 13 to 15 of the patent specification

III. In a letter dated 26 January 2000 the respondent (opponent) requested that the appeal be dismissed and requested oral proceedings as an auxiliary measure.

A detailed argumentation was presented concerning lack of inventive step of the subject-matter of all independent claims according to the appellant's main request as well as the first, second and third auxiliary requests.

Reference was in particular made to the following documents:

D1: US-A-4 453 074

D2: DE-A-36 10074

D5: D.E. Denning, "Digital Signatures with RSA and other Public-Key Cryptosystems", Communications of the Association of Computing Machinery, vol. 27, No. 4, April 1984, New York, USA, pages 388-392

IV. Claim 1 as granted, included in the main request as well as in all auxiliary requests, reads as follows:

"1. A system for issuing authorized personal identification cards (10) and for preventing unauthorized use thereof, comprising:
issuing terminal means (76) for issuing a plurality of personal identification cards (10); each of said cards having stored therein a first data string (20) with a portion (20a) thereof derived from a physical characteristic of an authorized user of the card, each of said cards (10) also having stored therein a signature (22) derived from a second data string (Q) using a private key (P1,P2) of a public-key cryptosystem pair, the public-key cryptosystem pair also having a public key (M), the second data string (Q) being derived from the first data string (20) using a predetermined one-way function (F) and having a length substantially less than the length of the first data string (20); and
transaction terminal means (78) including at least one transaction terminal for receiving a personal identification card (10) offered to effect a transaction using the transaction terminal, the personal identification card (10) having the first data string (20) and a received signature (22) stored therein, wherein the transaction terminal (78) comprises means, using the public key (M) of the public-key cryptosystem pair, for verifying that the received signature (22) can be generated from the first data string (20), means responsive to the verifying means for generating a representation from the first data string, and means for displaying (96) the representation and an indication of whether the

received signature (22) can be generated from the first data string (20) to enable an operator of the transaction terminal (78) to verify that the user of the offered personal identification card (10) is authorized to effect a transaction."

V. The appellant argued essentially as follows:

Document D1 was, like the patent in suit, directed to solving the problem of fraudulent use of intelligent data cards. In D1 this was done by encrypting a concatenation of a user password and a reference text using the private key of a public-private key pair and storing the encrypted data on the card. At the transaction terminal this data on the card was decrypted using the public key. However, the system of document D1 required additionally that the user of the card inputted the password in the transaction terminal, which was then compared with the password decrypted from the card. This was opposite to the claimed invention, which applied a one-way function so that the data stored on the card could not be decrypted back to the user password. Furthermore, in contrast to the claimed invention, in the system of document D1 the validity of the user could not be checked by displaying a representation of the user characteristic data stored on the card, but instead the user had to input a password, even if this was a physical characteristic, which was then compared to the decrypted password.

Document D2 on the other hand, disclosed a system in which picture data of the user were stored on a card in a compressed form. However, D2 showed no security features which prevented the data stored on the card from being tampered with.

Furthermore, even if a skilled person were to consider a combination of documents D1 and D2, this would merely teach the use of the image data as the password, which would need to be decrypted and compared to an input password.

Moreover, the use of a one-way function as suggested in D5 was incompatible with the teaching of D1 because the use of a one-way function in D1 would not allow the decryption of the concatenated text to obtain the reference text.

VI. The respondent's arguments may be summarised as follows:

Regarding the main request, the system according to claim 1 constituted a simple aggregation of features of the systems known from documents D2 and D1, wherein the system of D1 was furthermore modified by the data compression system known from document D5. A combination of both systems was obvious for the skilled person, when wishing to verify the authenticity of the card and the data stored thereon, as well as the legitimacy of the card's user. For both aspects different measures were required, known from document D1 and D2, respectively. These measures did not affect each other, but rather solved the specific partial problems.

The subject-matter of the remaining independent claims 3, 4, 5 and 6 did not involve an inventive step for in substance the same reason given with respect to claim 1.

The first auxiliary request merely differed from the main request in that features of the generation of the signature were included in claim 6. However, since the skilled person would already have understood claim 6 of the main request to have these features, the same finding applied to the claim as amended.

For the second and third auxiliary requests it was not seen how the deletion of some of the independent claims could positively affect the patentability of the remaining claims.

Reasons for the Decision

1. The appeal is admissible.

2. *Main request*

2.1 Claim 1

2.1.1 Claim 1 is directed to a system for issuing authorized personal identification cards and for preventing unauthorized use thereof; comprising:

(a) issuing terminal means (76) for issuing a plurality of personal identification cards (10),

(b) each of said cards having stored therein a first data string (20) with a portion (20a) thereof derived from a physical characteristic of an authorized user of the card,

(c) each of said cards also having stored therein a signature derived from a second data string (Q) using a private key (P1,P2) of a public-key cryptosystem pair, the public-key cryptosystem pair also having a public key (M),

(d) the second data string (Q) being derived from the first data string (20) using a predetermined one-way function (F) and having a length substantially less than the length of the first data string (20); and

(e) transaction terminal means (78) including at least one transaction terminal for receiving a personal identification card (10) offered to effect a transaction using the transaction terminal,

(f1) the personal identification card (10) having the first data string (20) and

(f2) a received signature (22) stored therein,

(g) wherein the transaction terminal (78) comprises means, using the public key (M) of the public-key cryptosystem pair, for verifying that the received signature (22) can be generated from the first data string (20),

(h) means responsive to the verifying means for generating a representation from the first data string, and

(i1) means for displaying (96) the representation and

(i2) an indication of whether the received signature (22) can be generated from the first data string (20) to enable an operator of the transaction terminal (78) to verify that the user of the offered personal identification card (10) is authorized to effect a transaction.

In accordance with the submission of the respondent, document D2 may be considered as representing the closest prior art.

From document D2 (cf. figures 1, 3 and corresponding description), in accordance with the terminology of claim 1 under consideration, a system is known for issuing authorized personal identification cards and for preventing unauthorized use thereof; comprising:

– issuing terminal means for issuing a plurality of personal identification cards,¨

– each of said cards having stored therein a first data string with a portion thereof derived from a physical characteristic (ie picture) of an authorized user of the card,

– transaction terminal means including at least one transaction terminal for receiving a personal identification card offered to effect a transaction using the transaction terminal,

– the personal identification card having the first data string stored therein,

– means for generating a representation from the first data string, and

– means for displaying the representation to enable an operator of the transaction terminal to verify that the user of the offered personal identification card is authorized to effect a transaction.

Thus, from document D2 a system is known comprising in substance the features (a), (b), (e), (f1), (h) and (i1) of claim 1 as listed above.

The claimed system differs from the one known from document D2 in that in addition protection is provided against fraudulent manipulation of the data string stored on the card. This is accomplished by storing a digital signature on the card obtained by encrypting the data string stored on the card at the issuing terminal and verifying the authenticity of the data string with the aid of this digital signature at the transaction terminal.

In the light of the above, the objective problem to be solved in the present case resides in the prevention against fraudulent manipulation of the data stored on the card. In the technical field at issue of secure card systems the formulation of this problem to be solved as such is obvious.

The solution to this problem in accordance with claim 1 (cf features (c), (d), (f2), (g) and (i2) of claim 1 as listed above) consists of:

– each of said cards also having stored therein a signature derived from a second data string (Q) using a private key (P1,P2) of a public-key cryptosystem pair, the public-key cryptosystem pair also having a public key (M),

– the second data string (Q) being derived from the first data string using a predetermined one-way function (F) and having a length substantially less than the length of the first data string,

– the personal identification card having the signature stored therein,

– wherein the transaction terminal comprises means, using the public key (M) of the public-key cryptosystem pair, for verifying that the signature can be generated from the first data string, and

– means for displaying an indication of whether the signature can be generated from the first data string.

As noted by the respondent, the wording for defining the verification of the authenticity of the signature and the first data string as used in the last two features above is inaccurate. It is clear that in the public-key cryptographic authentication schemes at issue, the public key is not used in the transaction terminal to generate the signature. Furthermore, it is evident that in this verification the one-way function has to be used as well. As a matter of fact, the verification involves verifying, using both the one-way function (F) and the public key (M) of the public-key cryptosystem pair, whether the decrypted signature, obtained by decrypting using the public key, corresponds to the second data string, obtained by applying the one-way function to the first data string. It is clear that the above two features should be construed accordingly.

Document D1 (cf column 4, line 14 to column 5, line 57) discloses a protection system for cards preventing fraudulent manipulation of the data on the card. According to an embodiment, the data string stored on the card comprises a set of numerical data derived from physiological attributes, such as a signature, voice sample or fingerprint of the legitimate card user (cf. column 1, lines 31 to 34) and a reference text. This data is encrypted by public-key cryptography using the private key in an initialisation terminal. The encrypted data, also named "digital signature", is also stored on the card. At the transaction terminal the encrypted data stored on the card is decrypted using the public key and compared with the data string stored on the card. A correspondence between the data proves

the authenticity of the data string. Accordingly, document D1 shows in substance the above features (c), (f2), (g) and (i2) of claim 1.

Document D5 (cf Chapter 5, "An improved signature scheme") discloses a further improvement in public-key cryptography used for generating digital signatures for certifying the authenticity of data. Before encrypting the data using the private key, the data is transformed using a one-way hashing function. At the transaction terminal the same (public) one-way hashing function is applied to the data string stored on the card. The encrypted data stored on the card is decrypted using the public key and now compared with the hashed data string. The use of the one-way hashing function improves the security of the system and has the additional advantage of producing hashed data having a reduced length compared to the initial data string thereby speeding up the public key transformation. Accordingly, document D5 shows the above feature (d) and the use of the one-way function in the feature (g) of claim 1.

It would have been obvious to the skilled person, seeking a solution to the above problem of preventing fraudulent manipulation of the data stored on the card as provided by document D2, to apply the teachings of documents D1 and D5 providing a straightforward solution to this problem, thereby arriving at the subject-matter of claim 1 under consideration.

2.1.2 The argument presented by the appellant, and in substance set out by the opposition division in its further remarks concerning claims 1 and 3, according to

which the use of the one-way function in D5 was incompatible with the teaching of D1 because the use of the one-way function in D1 would not allow the decryption of the concatenated text to obtain the reference text, is not convincing.

True, with the improved public key authentication system using a one-way hashing function as suggested in D5, the decryption of the data on the card at the receiving end yields the hashed data and not the initial data. Accordingly, when applied to the system of document D1, the decryption of the data on the card at the receiving end would yield the hashed form of the reference text. However, as pointed out by the respondent, document D5 teaches that in this case, at the receiving end the same (public) hashing function should be applied to the reference text first, and the resulting hashed form of the reference text compared with the outcome of the decryption of the data on the card. The reference text would invariably fulfil its role of rendering the system secure as suggested in document D1 (cf column 5, lines 3 to 66). Accordingly, there is no incompatibility between the teachings of document D1 and D5 in this respect.

Merely for the sake of completeness, it is noted that the remark of the opposition division that the semantic meaning of the reference text was an essential feature of D1, is unfounded. In the system of D1 the reference text is stored in every transaction terminal and compared by the terminal with the result after decryption of the data on the card for correspondence. The reference text is simply a data string with no requirements concerning its semantic meaning.

The appellant also relied on the argument that in contrast to the claimed invention, in the system of document D1 the validity of the user could not be checked by displaying a representation of the user characteristic data stored on the card, but instead the user had to input a password, even if this was a physical characteristic, which was then compared to the decrypted password. Furthermore the appellant argued that the system of document D1 required additionally that the user of the card inputted the password in the transaction terminal, which was then compared with the password decrypted from the card. This would be opposite to the claimed invention, which applied a one-way function so that the data stored on the card could not be decrypted back to the user password.

However, as pointed out by the respondent, in document D1 (cf column 1, lines 40 to 52, column 4, lines 14 to 56) both the password as such and the encrypted password (ie the encryption of both the password and the reference text) are stored on the card. At the transaction terminal the card user is required to input his password. If the password is for instance derived from a physical characteristic like a picture of the authorised user, a device such as a camera at the transaction terminal would produce the corresponding derivate defined as the password. Two different security checks are now performed at the transaction terminal. In a first check the password stored on the card is verified for a match with the inputted password, which for physiologically derived passwords means an acceptable resemblance rather than an exact coincidence. This check serves to verify that the card

belongs to the user. In a second check the encrypted data stored on the card is decrypted so as to obtain the password and the reference text, which are then verified for a match with the inputted password and the reference text stored in the transaction terminal, respectively. This second check serves to verify that the card is authentic and the data stored thereon has not been tampered with.

In the system according to claim 1, a representation is generated from the data string stored on the card and displayed to enable an operator of the transaction terminal to verify that the user of the offered card is authorised to effect a transaction. However, for the purpose of this verification the operator must dispose of a reference image of the user at the transaction terminal, such as for instance a video image of the user. This input, however, corresponds to the input of a physiologically derived password at the transaction terminal envisaged in document D1.

Admittedly, in the system of document D1 the validity of the user is verified by an acceptable resemblance between for instance the picture of the user obtained with the analytical device at the transaction terminal and the data stored on the card, as assessed by the, mostly unattended, terminal, rather than by an operator as is the case in the claimed system. However, document D2 already shows a system, in which the validity of the card user is verified by an operator assessing the resemblance between a picture stored on the card and a video image of the user at the terminal. Moreover, displaying the data stored on the card for assessment by an operator, as suggested in D2, is not in conflict

with the teaching of document D1 for physiologically derived passwords, since physical characteristic data such as a picture of the user, are typically not "secret".

As far as the verification of the inputted password is concerned, as discussed above with respect to document D5, the use of a system based on a one-way hashing function would require that rather than comparing the inputted password with the decrypted data, the one-way hashing function is first applied to the inputted password and the result is compared with the decrypted data. Accordingly, the teaching of document D1 is not opposite to the claimed invention, but rather, when complemented with the improved security feature provided by the one-way hashing function as suggested in document D5, and when applied to a system as known from D2, results in a system in accordance with claim 1.

2.1.3 Thus, for the reasons given above the subject-matter of claim 1 lacks an inventive step.

2.2 The subject-matter of the remaining independent claims 3, 4, 5 and 6 lacks an inventive step for in substance the same reasons given above with respect to claim 1.

2.3 Accordingly, the main request is not allowable (Articles 52(1), 56 and 100(a) EPC).

3. *First, second and third auxiliary requests*

The first, second and third auxiliary requests all include claim 1 discussed above, which was found to lack inventive subject-matter, and fail accordingly (Articles 52(1), 56 and 100(a) EPC).

4. The present decision is based on grounds and evidence submitted by the respondent, on which the appellant has had ample opportunity to present comments in accordance with Article 113(1) EPC. Since the appellant has not requested oral proceedings, the case is ready for decision. The issue of a provisional opinion as a communication under Article 110(2) EPC is neither necessary nor appropriate under these circumstances (cf Schulte, Patentgesetz mit EPÜ, 6th edition, page 987, nr 22).

Order

For these reasons it is decided that:

The appeal is dismissed.

The Registrar: The Chairman:

D. Sauter G. Davies